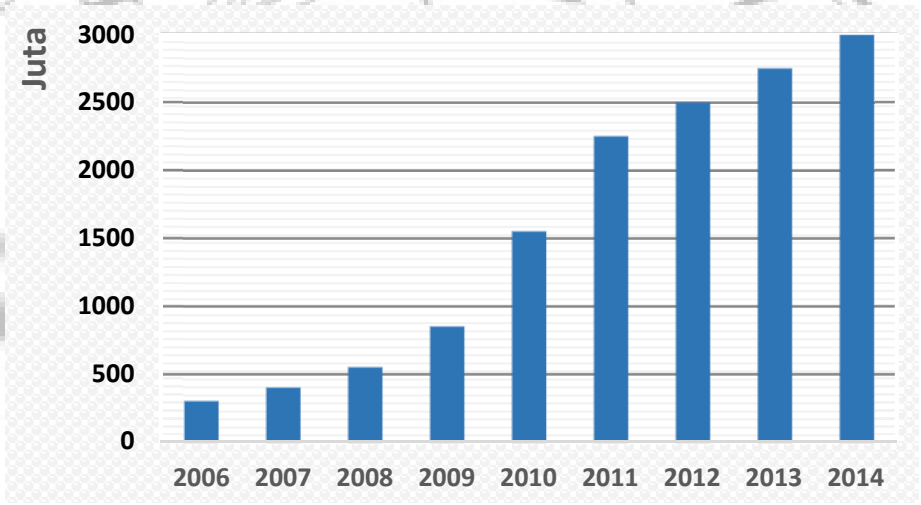
BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring meningkatnya ilmu pengetahuan dan perkembangan teknologi informasi, akses data dalam jaringan menjadi sangat mudah. Salah satu kemudahan dalam teknologi pada era ini adalah internet, dapat ditunjukkan pada **Gambar 1.1**, orang sangat bergantung pada internet untuk menyebarkan informasi yang berharga [1]. Di sisi lain, karena ketergantungan yang tinggi pada internet, beberapa orang memanfaatkan kelemahan internet untuk memberikan gangguan kepada pengguna lainya.



Gambar 1.1 Jumlah Pengguna Internet hingga 2014
Sumber: Bhattacharyya dan Kalita [1]

Gangguan terjadi karena adanya pihak yang ingin menyerang, merusak, bahkan mengambil data-data penting. Gangguan tersebut umumnya diketahui dari gejala aneh yang terjadi. Kurangnya informasi tentang penyerang seperti siapa yang menyerang, mengapa mereka menyerang, bagaimana mereka menyerang, dan kapan serangan dilakukan, menjadi masalah yang patut untuk dicermati.

Untuk menangani hal tersebut, dibutuhkan alat bantu untuk mendeteksi serangan yang masuk ke dalam jaringan. Salah satu alat bantu dalam keamanan

jaringan yang bisa digunakan adalah *honeypot*. *Honeypot* merupakan sistem yang sengaja digunakan dengan harapan untuk diserang dan dieksploitasi [2]. *Honeypot* mempunyai nilai tambah dalam penelitian untuk mempelajari ancaman dan resiko keamanan jaringan. *Administrator* dapat menganalisa aktivitas penyerang menggunakan *honeypot*. Secara umum, *honeypot* dibagi menjadi tiga tingkat, yaitu *low interaction, medium interaction* dan *high interaction*. Semakin tinggi tingkat interaksi pada *honeypot*, maka semakin besar data yang ditangkap dan semakin besar juga resiko yang diterima [3].

Biasanya *honeypot* diimplementasikan menggunakan satu komputer *desktop* atau lebih, namun dalam penelitian ini *honeypot* akan dipasang pada *raspberry pi*. Keuntungan menggunakan *raspberry pi* antara lain mempunyai harga yang relatif lebih murah dan mengkonsumsi daya yang lebih sedikit daripada menggunakan komputer *desktop* [4]. *Raspberry pi* dapat digunakan sebagai sensor *honeypot* untuk pemantauan keamanan jaringan menggantikan komputer *desktop* pada umumnya [5]. Selain itu, *raspberry pi* mudah disesuaikan, dan bisa diletakkan dimana saja karena ukurannya yang cukup kecil.

Seiring dengan sulitnya menganalisis *log* yang dihasilkan oleh *honeypot*, maka dibutuhkan alat visualisasi untuk mempermudah dalam menganalisis *log honeypot*. Dalam penelitian ini, hasil serangan *honeypot* divisualisasikan menggunakan *ELK stack*, dimana *ELK stack* ini adalah kombinasi dari *elasticsearch, logstash* dan *kibana* [6]. Berdasarkan uraian latar belakang masalah tersebut, judul yang akan dipakai dalam penelitian ini yaitu "Implementasi *Multiple Honeypot* dengan *Raspberry Pi* dan Visualisasi *Log* mengunakan *ELK Stack*".

1.2 Rumusan Masalah

Beralaskan latar belakang masalah diatas, adapun rumusan masalah di dalam penelitian ini adalah:

1. Bagaimana cara implementasi multiple *honeypot* pada *raspberry pi?*
2. Bagaimana penerapan *ELK stack* untuk visualisasi hasil laporan *honeypot?*
3. Apakah sistem yang dirancang mampu mendeteksi serangan yang masuk ke dalam jaringan?

1.3 Batasan Masalah

1. Penelitian ini hanya membahas implementasi *honeypot* menggunakan *cowrie*, *dionaea*, dan *suricata*.
2. Penelitian ini berfokus pada bagaimana cara implementasi beberapa *honeypot* pada *raspberry pi* dan memvisualisasikan hasil *log honeypot* pada ELK *stack.*
3. Pengujian serangan menggunakan *scanning*, serangan *brute force*, serangan *metasploit* dan serangan DoS.
4. Perangkat lunak yang digunakan untuk pengujian yaitu perangkat yang sudah tersedia dan berbasis *opensource*.
5. Serangan yang dilakukan hanya dalam jaringan lokal saja (*Local Area Network*).
6. Teknik pengujian pada penelitian ini menggunakan pengujian *black box*.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang akan dilakukan yaitu untuk merancang sistem yang mampu mendeteksi serangan pada jaringan menggunakan *honeypot*. Penelitian ini akan memberikan hasil laporan *honeypot* dalam bentuk visualisasi untuk mempermudah dalam meganalisis hasil yang didapatkan oleh *honeypot*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberi manfaat antara lain:

1. Sebagai syarat untuk mendapatkan gelar sarjana bagi penulis.
2. Memberikan peringatan awal bagi administrator dalam menjaga, dan melakukan tindakan pencegahan keamanan jaringan secara *real time.*
3. Sebagai alat penelitian untuk mengetahui tingkah laku serangan pada keamanan jaringan.

1.6 Metodologi

Penelitian dilakukan dengan menggunakan beberapa metode penelitian, diantaranya:

1.6.1 Studi Pustaka

Dalam penelitian ini, penulis melakukan studi pustaka dari berbagai literatur termasuk dari buku, makalah-makalah, artikel ilmiah, maupun materi-materi dari internet yang searah dengan penelitian ini. Sumber pustaka antara lain berhubungan dengan kemanan jaringan, *dionaea honeypot, suricata honeypot, cowrie honeypot, ELK stack, raspberry pi, scanning port, brute force*, *malware*, dan DoS.

1.6.2 Desain Sistem (Perancangan)

Berdasarkan studi pustaka yang telah dilakukan, dapat ditentukan bagaimana rancangan yang akan dibuat. Pada tahap ini, penulis merancang desain sistem yang nantinya akan diimplementasikan.

1.6.3 Implementasi Sistem

Pada tahap ini dilakukan implementasi sesuai dengan perancangan sistem yang telah dibuat, dimulai dari instalasi perangkat lunak yang akan dipakai dan konfigurasi pada sistem.

1.6.4 Pengujian Sistem

Pengujian ini digunakan untuk mengetahui apakah hasil dari perancangan dan implementasi sudah berjalan sesuai dengan tujuan penelitian.

1.6.5 Sistematika Penulisan

Pada sistematika penulisan dijelaskan secara menyeluruh permasalahan yang akan dibahas. Untuk memudahkan penulisan, sistematika penulisan dibuat menjadi lima bagian, antara lain:

BAB I PENDAHULUAN

Bab ini mencakup latar belakang penelitian yang berjudul *"Implementasi Multiple Honeypot dengan Raspberry pi dan Visualisasi Log Honeypot Menggunakan* ELK *Stack",* rumusan dari permasalahan, batasan masalah, manfaat penelitian, tujuan penelitian, metode penelitan dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini mencakup teori-teori, informasi, dan kajian penelitian sebelumnya yang berkaitan dengan lingkup penelitian yang dilakukan. Tinjauan pustaka digunakan penulis sebagai rujukan penulis pada saat melakukan penelitian dan mengemukakan argumen pada hasil penelitian.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini mencakup analisis masalah, kebutuhan perangkat keras dan lunak yang digunakan. Selain itu dijelaskan beberapa perancangan yang akan diimplementasikan, perancangan tersebut meliputi rancangan sistem dan skenario pengujian.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini mencakup implementasi dari perancangan sitem dan pengujian terhadap sistem. Tahap ini dilakukan setelah sistem didesain dan dianalisis pada perancangan sistem. Teknik pengujian yang dipakai dalam pengujian ini yaitu pengujian *black box.*

BAB V PENUTUP

Bab ini mencangkup kesimpulan yang bisa diambil berhubungan dengan sistem yang dibuat dan saran untuk meningkatkan sistem lebih lanjut.


UNIVERSITAS MUHAMMADIYAH
MALANG